

PCT/JP 99/02599

EAKU

日 本 国 特 許 庁

19.05.99

PATENT OFFICE  
JAPANESE GOVERNMENT

2999/2099

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1998年12月21日

出 願 番 号

Application Number:

平成10年特許願第361752号

出 願 人

Applicant (s):

保倉 豊

REC'D 09 JUL 1999

WIPO PCT

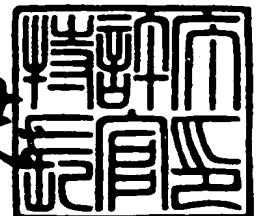
PRIORITY  
DOCUMENT

SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

1999年 6月17日

特許庁長官  
Commissioner,  
Patent Office

伴佐山 建志



出証番号 出証特平11-3041203

【書類名】	特許願
【整理番号】	GFS0004
【あて先】	特許庁長官 殿
【国際特許分類】	H04L 9/32 G06K 19/00
【発明の名称】	認証 I C カード
【請求項の数】	7
【発明者】	
【住所又は居所】	千葉県八千代市勝田台南 2 丁目 1 5 番 2 2 号
【氏名】	保倉 豊
【特許出願人】	
【識別番号】	398035796
【氏名又は名称】	保倉 豊
【代理人】	
【識別番号】	100104341
【弁理士】	
【氏名又は名称】	関 正治
【電話番号】	03-3234-4241
【手数料の表示】	
【予納台帳番号】	041232
【納付金額】	21,000円
【提出物件の目録】	
【物件名】	明細書 1
【物件名】	図面 1
【物件名】	要約書 1
【プルーフの要否】	要

【書類名】 明細書

【発明の名称】 認証 IC カード

【特許請求の範囲】

【請求項 1】 CPU と、人証情報もしくは人証情報と認証情報を格納した認証ファイルと、認証の深さに応じて分類されたジョブプログラムやデータを格納したアプリケーションファイルとを備え、外部から前記アプリケーションファイルへのアクセスの要求があったときに、前記認証ファイルに格納された人証情報に基づいて真偽を判定した結果により該アクセスを認める認証 IC カードであって、前記認証ファイルにカードで認証する第 1 の人物以外に少なくとも 1 人の第 2 の人物の人証情報または少なくとも 1 つの主体の認証情報を格納し、該第 2 人物または主体の認証を要求するジョブあるいはデータを予め決めてあって、該第 2 人物または主体の認証を要求するジョブあるいはデータについて実行あるいは提示の要求があったときに、前記第 2 人物または主体によって外部から入力される人証情報または認証情報と前記認証ファイルに格納された人証情報または認証情報とを対比して認証に合格したときに前記 CPU を介して前記ジョブの実行やデータの提示を認めるようにしたことを特徴とする認証 IC カード。

【請求項 2】 前記 CPU が認証の合否を決定することを特徴とする請求項 1 記載の認証 IC カード。

【請求項 3】 前記 CPU が前記認証ファイルに格納された人証情報または認証情報を外部装置に出力して、該外部装置から受け取る判定結果に基づいて、前記 CPU を介して前記アプリケーションファイルへのアクセスを行うことを特徴とする請求項 1 記載の認証 IC カード。

【請求項 4】 前記人物または主体の認証を前記第 1 人物および前記第 2 人物または前記主体の両者について実行して両者共に合格したときに始めて前記アプリケーションファイルへのアクセスが認められるようにしたことを特徴とする請求項 1 から 3 のいずれかに記載の認証 IC カード。

【請求項 5】 前記人証情報が該 IC カードの真正な所有者の個体を区別する生物学的情報を含むことを特徴とする請求項 1 から 4 のいずれかに記載の認証 IC カード。

【請求項 6】 さらに前記第 2 人物または前記主体の認証を利用した事項についてのログを記録するようにしたことを特徴とする請求項 1 から 5 のいずれかに記載の認証 IC カード。

【請求項 7】 さらに前記認証 IC カードが認証の内容を記録した電子証明用ファイルを有し、前記アプリケーションファイルへのアクセスを行うときに利用された認証の内容を表す電子証明書を提示することができるようにしたことを特徴とする請求項 1 から 6 のいずれかに記載の認証 IC カード。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、電子情報交換や電子商取引における個人認証を行うため認証票として用いる認証 IC カード、あるいは格納した個人情報提示するときに適切な保護ができるようにした認証 IC カードに関する。

【0002】

【従来の技術】

認証 IC カードは、研究所や事業所、研究室、資料保管室さらに住宅など、特定の場所に入出りできる者を限定し、セキュリティを高めるために有効である。また、商品の販売やクレジットなどの電子商取引、医療におけるオンライン診察、個人カルテや役所における登録事項の閲覧、証明書の発行など、本人にのみ取引を認めるべき場合に本人認証を正確に行う目的で使用する事ができる。

このような認証 IC カードは、カードに記録された情報に基づいて本人認証をおこなうため、カードのセキュリティが大きな問題となる。

【0003】

特に、既に本願出願人の出願に係る特願平 10-299181 号公報に開示されたような、使用者本人の人証情報を IC カードに記憶させて取引における人証に用いる認証 IC カードでは、IC カードに記録された情報とカード所有者本人が入力する情報のみに基づいて認証を行うことができるようになっている。したがって、カードのセキュリティはこれまでも増して重要になるので、真正な取引対象者の署名、声紋、指紋、掌紋、虹彩などの生物学的情報や自由度の大きい

暗証番号などを利用して、真正な取引対象者以外の者が認証カードの利用をできないようにする高度な安全確保手段が準備されており、正当利用者でない他人が窃取や拾得などにより取得した認証 IC カードを直接利用したり改竄して利用することができない。

【0004】

しかし、人証情報を忘れた場合に備えて本人には記録した人証情報を教える手段を用意し、また自身の都合により人証情報の書き換えを認めることが必要になるので、こうした手段を利用して本人以外の者が係員を騙したり係員と結託して不正に入手した人証情報を悪用することもあり得る。

また、不正に取得した人証情報を使って IC カードを書き換えたり、あるいは新しい IC カードを使って他人の認証カードを偽造するような犯罪行為を完全に防止することはできない。

このように、安全性を高めた認証 IC カードでも、使用システムに精通した者や内部の者が悪意をもって改竄や偽造することまで防ぐことは困難であった。

【0005】

【発明が解決しようとする課題】

そこで、本発明が解決しようとする課題は、極めて高度なセキュリティを有する認証 IC カードを提供することである。特に、カード自体に正当利用者の人証情報を記録して用いる認証 IC カードにおけるセキュリティをさらに高めることである。

【0006】

【課題を解決するための手段】

上記課題を解決するため、本発明の認証 IC カードは、CPU と、人証情報あるいは人証情報と認証情報を格納した認証ファイルと、認証の深さに応じて分類されたジョブプログラムやデータを格納したアプリケーションファイルとを備え、外部からアプリケーションファイルへのアクセスの要求があったときに、認証ファイルの人証情報または認証情報に基づいて真偽を判定した結果によりアクセスを認める認証 IC カードであって、認証ファイルに正当利用者自身の人証情報に加えて第 2 人物の人証情報あるいは主体の認証情報を格納し、第 2 人物あるい

は主体の認証を要求するジョブあるいはデータを予め指定してあって、このような指定のジョブあるいはデータについて実行あるいは提示の要求があったときには、外部から入力される人証情報や認証情報を認証ファイルの人証情報や認証情報と対比して認証に合格したときにCPUを介して指定のジョブの実行やデータの提示を認めるようにしたことを特徴とする。

## 【0007】

本発明の認証ICカードによれば、指定したジョブやデータにアクセスするためには、認証ICカードの正当使用者に加えて特定の権限を有する第2人物あるいは主体（以下、立会人という）の承認が必要になるため、特に認証ICカード自体の正当性や使用者の正当性についての確認が重要な問題となるようなジョブなどを指定しておけば、極めて高度なセキュリティを確保することができる。

なお、立会人の承認はICカードに記憶された人証情報あるいは認証情報に基づいて認証されたときに始めて有効になる。

## 【0008】

たとえば、認証ICカードを発行するときに1人または2人以上の立会人を立て、この人物等の人証情報や認証情報を併せて認証ICカードに記録して使用するようにすることができる。このようなカードを使用し、たとえ使用者の要求があってもこの立会人の承認がない限り、一旦入力された本人人証情報を再度見ることができないようにしたり人証情報や認証情報の書き換えを許さないようにする。なお、立会人は使用者の信認する第三者であってもカード発行責任者の指定する者であってもよい。また、機構や組織としての発行者などの主体であってもよい。

## 【0009】

このようなシステムでは、本人でない立会人の承認と認証がなければならず、あるいは本人と立会人が共に揃って認証に合格しなければならないから、窃取者が偽って人証情報の開示を受け認証ICカードを盗用することを防ぐことができるばかりでなく、内部情報に明るい係員が結託して人証情報を書き換えたりすることをも防ぐことができる。

また、認証ICカードの信頼性に係る認証に高いセキュリティを設定すること

ができるため、認証 IC カードを発行するカード発行所に特別なセキュリティシステムがなくても認証 IC カードの安全性は脅かされることがない。またカードに記憶する個人に関するデータは認証 IC カードの中に格納すればよく、認証 IC カード発行所に残しておく必要がない。

したがって、信用水準の高いカード発行システムをより容易に構築することができる。

#### 【0010】

なお、認証の可否は認証 IC カード内の CPU であっても、外部装置であってもよい。外部装置を使用する場合は、CPU を経由して認証ファイルに格納された人証情報または認証情報を外部装置に出力し、外部装置で認証の可否を判定し合格したときに始めて、CPU を介してアプリケーションファイルへのアクセスを行う。

認証の可否を認証 IC カード内の CPUで行うようにした場合は、IC カード読み取り装置側の設備が簡単でよくなり、使用場所における設備費を節約することができる。

また、外部装置で行うときは、IC カードの性能を簡単化することができる。また、人証情報の一部を認証 IC カード以外の記憶装置に分担して持たせることにより安全性をさらに向上させるシステムに対する適合性がよい。

#### 【0011】

なお、人証情報は認証 IC カードの真正な所有者の個体を区別する生物学的情報を含むようにすることが好ましい。生物学的情報には、署名、声紋、指紋、掌紋、虹彩などがある。ただし、生物学的情報以外にも自由度の大きい暗証番号などを利用することも可能であることはいうまでもない。

また、さらに立会人の認証を利用した事項についてのログを認証 IC カード内に記録するようにすることが好ましい。

何らかの事故が発生したときに、その状況を把握したり原因を推定するのに役立つからである。

#### 【0012】

#### 【発明の実施の形態】

以下、本発明の詳細を図面を参照して実施例に基づいて説明する。

図1は本発明の実施例である認証ICカードの構成を示すブロック図、図2から図4は本実施例の使用例を示す流れ図である。

本実施例の認証ICカードは、図1にあるように、演算処理を実行するCPU 1、演算処理プログラムを収納したROM 2、演算処理中のデータを記憶するRAM 3、データの書き込み読み出しが可能なデータ記憶装置4、アプレットプログラムに対するインターフェース5、外部接続用接続回路6、および外部接続端子7を備える。

#### 【0013】

外部接続端子7は、信号伝達および電源の供給に用いられるもので、非接触型の電極やアンテナであっても良い。また、各種のカード読み込み装置に対応するため接触型と非接触型の両方の接続端子を備えるようにしても良い。

アプレットインターフェース5は、CPUを作動させる小型プログラム（アプレット）を外部から受け入れるときに用いるもので、受け取ったアプレットを認証ICカードで機能させるためのインターフェースである。安全のためアプレットを受け付けないようにした認証ICカードではアプレットインターフェース5を備える必要はない。

#### 【0014】

データ記憶装置4のファイルには、認証データを記憶した認証ファイル10と、特定のジョブを実行するためのジョブプログラムや各種データを格納したアプリケーションファイル20が含まれる。

認証ファイル10には、認証ICカードが真正であることを保証するためのデータに加えて、認証ICカードの真正な所有者を認証するための人証情報が格納されている。

#### 【0015】

人証情報は、たとえば暗証番号、指紋、声紋、顔写真、サイン筆跡など、本人しか知らないものや生物学的情報で本人以外では再現できないようなものが好ましい。認証情報は1種に限らず多数種類格納しておいて1個単独でもしくは複数個を複合して使用することができる。



認証ファイル 10 には、認証 IC カードにより認証する真正な所有者の人証情報を記憶した第 1 人証ファイル 11 と、保証人や立会人あるいは発行人などの第 2 の人物に関する人証情報や主体に関する認証情報を記憶する第 2 人証ファイル 12 とが含まれている。これら第 2 人物や主体などの立会人はシステム上の必要に応じて 2 人以上の人物や主体であってもよい。

【0016】

アプリケーションファイル 20 は、認証 IC カードの真正性に関する情報を扱う部分が格納された第 1 作業ファイル 21 と、認証結果に基づいて実行するための部分が格納されている第 2 作業ファイル 22 を含む。

第 2 作業ファイル 22 には、例えば住宅管理用情報、医療情報、金融情報、通信情報など、認証を使用するサービス機関毎に必要なとされる情報が、暗証番号など簡単な認証でアクセスを認めるものから、指紋で確認するなど高度な認証に合格して始めてアクセスを認めるものまで、要求される認証の程度に従って分類された状態で格納されている。なお、暗号の鍵や電子証明書などを入れておくこともできる。また、開錠指示を発するジョブなどのプログラム類を格納しておいてもよい。

【0017】

また、第 1 作業ファイル 21 には、人証情報を書き込むジョブや、人証情報の読み出しや書き換えを行うジョブ、あるいはログの読み出しや消去を行うジョブなど、認証 IC カードの真正性に係わるジョブや情報が格納されている。

第 1 作業ファイル 21 に格納したジョブや情報は、要求される機密水準に基づいて、所有者のみ認証すればよいものと、第 2 人物のみ認証すればよいものと、所有者と第 2 人物の両方を認証しなければならないものとに分けておくことができる。

【0018】

図 2 から図 4 を参照して本実施例の認証 IC カードの使用例を説明する。

図 2 は、認証 IC カードを発行するときの手順を例示するものである。

認証 IC カードの発行要求があると (S11)、カードの発行者は認証カードの認証対象者の信用審査をし (S12)、この審査に合格して認証対象者が認証

カードを正当に使用できる者であると認定できるときは、認証対象者の保証ができる人あるいは認証対象者が信頼する人を立会人として指名させる（S 13）。

【0019】

認証 IC カードを発行するときには、指定のカード発行所に関係者全員が集合して（S 14）、認証 IC カードとカード発行装置が互いに真正であることを確認して（S 15）、認証 IC カードの発行を認めると（S 16）、各人が人証情報を入力する（S 17）。

なお、認証 IC カードにカード読み取り器が真正なものであることを確認する機能を持たせるのは、認証 IC カードに格納されている情報を窃取したり内容の書き換えをすることを防ぐ必要があるからである。

【0020】

カード所有者になる人は、カードに基づいて取引するとき取引に要求される信用度が異なることに対応して、暗証番号、独自の記号、サイン、指紋、声紋、虹彩、掌紋など幾つかの人証情報を入力する。立会人についても複数の人証情報を入力させてもよいが、立会人の認証が必要となるケースは限られているので、幾つもの人証情報を使用する必然性はない。なお、立会人は組織や機構としての主体であってもよく、この場合には生物学的情報の代わりに電子サインのような認証情報により認証を行うようにすることができる。

【0021】

なお、認証 IC カードは社内で種々の権限を確認するために使用する場合もあるが、このような場合に例えば発行を担当する人事部などの部局の責任者や発行担当係員が上記カード発行者や立会人として認証を受けるようにしてもよい。あるいはカードを所持する人物の属する部局の責任者が認証を受けるようにしてもよい。

【0022】

入力された所有者本人の人証情報は認証 IC カード中の第 1 人証ファイル 11 に格納し、立会人等の人証情報や認証情報は第 2 人証ファイル 12 に格納する。また、認証を行ったときにその認証の信頼性や根拠を記載した電子証明書を要求されることがあるが、このような認証 IC カードが発行することになる電子証明

書は各種の取引類に用いられるアプリケーションデータと共にアプリケーションファイル20中の第2作業ファイル22に格納される（S18）。

【0023】

なお、認証ICカードに記録された人証情報を表示させたり書き換えを行うためのプログラムは第1作業ファイル21に格納されており、アクセスするためにはそれぞれのジョブに対応して予め決められた認証を満足しなければならない。

上記のように、必要な情報を書き込んだ認証ICカードは、認証対象者が適正な人証情報を入力したときに適正な動作をすることなど、製品としての完成度を確認する適当なテストを受け（S19）、これに合格すると所有者に交付される（S20）。合格しない場合は、例えば認証情報等の書き込み工程（S18）をやり直して適正な認証ICカードにしてから交付する。

なお、発行主体の審査により（S12）カードの認証対象者がカードにより認証システムを利用するのに相応しくないと判定したときは認証ICカードの発行は拒絶されることになる（S21）。

【0024】

このような認証ICカードは、サービスや取引（代表して取引と呼ぶ）毎に利用資格を与えられた者が所持する認証ICカードにその取引を認めるための暗号信号を記録しておき、取引を行うときに認証ICカードの携帯者が真正な所持者であることを確認して取引を認める仕組みに用いることができる。

この場合に、取引者が認証ICカードから受け取るべき情報は、認証ICカードの携帯者がカードの真正な所有者であることと認証ICカードに利用資格を有する証拠となる暗号信号が記録されていることである。また、認証ICカードが認証することは、読み取り装置が適正なものであることと携帯者が真正な所持者であることである。

【0025】

この認証ICカードでは、建物への入場やある資料室への入室の資格、銀行の口座、クレジットの所有、さらに戸籍、履歴や、電子マネーとして利用する場合の与信残高などを含め、いわば所持者の属性を認証ICカードに収納することにより、利用資格が与えられた全ての取引の認証を1枚のカードに統合することが

できる。

【0026】

認証 IC カードの利用方法の代表的な例として住宅の入室管理に使用した例を挙げて説明する。

各室の扉には扉開閉制御装置が設備されていて、ここから発生される制御信号に従って扉の開閉が行われる。扉開閉制御装置には認証制御装置、人証情報入力装置、カード読み込み器が接続されている。

入室しようとするカード使用者が認証 IC カードをカード読み取り器に挿入すると、認証制御装置と認証 IC カードは ID を交換して互いに真正な組み合わせか否かを確認する。情報のやり取りは全て CPU を介して行われ、カード読み取り器は直接的に認証 IC カードのデータ記憶装置にアクセスできない。

【0027】

認証制御装置は、認証 IC カードがシステムに適合した真正なものであるときには、カードの使用者に認証レベルに基づいて決められた例えば指紋など、人証情報の入力を督促し、入力された情報を抽出処理して人証情報を作成する。

人証情報が真正であることを認証 IC カード側または扉開閉制御装置側で確認したときには、扉を開くための開扉暗号を発生して、扉開閉制御装置により扉を開ける。

【0028】

また、認証ファイルに格納される人証情報の数はいくつに設定しても良い。人証情報としては、カードの発行者が記入しておく ID 番号のみに基づいて真正を証明する最も簡単な段階から、カードの所有者が決めた暗証番号、所有者の指紋、虹彩、顔写真などの生体情報、所有者が入力するサインなどの動的情報、さらにこれらを組み合わせたより高度な複合情報などが使用できる。

このようにして、他人による成り澄ましが困難な信頼性の高い認証ができる。

【0029】

この認証 IC カードは多種類の人証情報を場合によって使い分けるようになっている。そこで、真正な所有者といえども自分が使用すべき人証情報を忘れてしまうことが間々ある。このような場合に、カードが使用できなくなるのでは不便

なので記録された人証情報を表示できるようにするのが普通である。

また、人証情報は他人に漏れて盗用されそうときや安全性を高めるために定期的に変更するときなど、所有者本人の必要により変更できるようにしておくことが好ましい。

#### 【0030】

したがって、認証 IC カードの構造に詳しく取り扱い機器を自由にすることができ人物が悪意を持って認証 IC カードに格納した情報を引き出して、カードを改竄したり、偽の認証 IC カードの作製を行おうとすれば、これを防止することは容易でない。

ところが、本実施例の認証 IC カードは予め決められたジョブについては立会人の認証を求めることができるから、認証 IC カードの認証情報にアクセスする場合には立会人の承認を要求することにしておけば、内部事情に詳しい者であっても人証情報を盗み出して利用したり人証情報を書き直したりすることができない。

#### 【0031】

図 3 は、真正な認証対象者が自己の人証情報を確認するときに要求される手順を示す流れ図である。

認証 IC カードの人証情報を読み出したいときは (S 31)、カードにより認証を受けるべき認証対象者とカード発行時の立会人とカード発行所の責任者あるいは組織としての主体が集合して (S 32)、カードが真正なものであるかを確認の上 (S 33)、それぞれ人証情報あるいは認証情報を入力する (S 34)。

#### 【0032】

それぞれの人物等の人証情報・認証情報を認証 IC カードに格納されている人証情報・認証情報と参照して一致していれば (S 35)、このようなアクセスがあったという事実を認証 IC カード内の記憶装置にログとして残し (S 36)、記録されていた人証情報をカード読み込み装置に付属するディスプレイに表示する (S 37)。必要な人証情報等が一致しない場合は不正なアクセスであるので、人証情報の表示を拒絶する (S 38)。

#### 【0033】

なお、カードの認証対象者は覚えている人証情報をひとつ入力し、これが認証 IC カードに格納されているもののひとつに一致していればよいとする。ここで、たとえば暗証番号を忘れたときは指紋の参照で開示するが、サインを知りたい場合には暗証番号が一致しても教えないようにするなど、表示を求める人証情報より高度の人証情報で認証できたときに限って表示するようにしてもよい。

また、高度な安全性を要求しない人証情報については、立会人等が集まらなくても、所有者本人の生物学的特徴に基づいた人証情報により本人認証ができれば開示するようにしてもよい。なお、特別な場合はカード発行責任者がその責任において独自に情報を読み出せるようにすることも可能である。

#### 【0034】

図4は、人証情報の書き換えを行うときの手順を表す流れ図である。

人証情報の書き換え要求があったときには（S41）、認証対象者本人だけの了承でよしとすると他人による不正使用を排除することができない場合があるので、立会人や発行担当者等を集めて（S42）全員が承認することを確認する。認証 IC カードと発行装置の真正性を互いに確認した後（S43）、集合した人物等のそれぞれが人証情報・認証情報を入力する（S44）。入力した人証情報等が認証 IC カード内に格納されている情報と一致するときに（S45）始めて人証情報の書き換えを許可する。

#### 【0035】

各人の認証に合格したときには、記録されていた人証情報を外部の記憶装置に転写し（S46）、書き換えの事実についてのログを認証 IC カード内に記録する（S47）。さらに、不要になった人証情報を消去し（S48）、所有者本人に人証情報を入力させ（S49）、新しい人証情報を認証 IC カードに格納する（S50）。

その後認証 IC カードの機能をテストして（S51）合格したら所有者に交付する（S52）。認証 IC カードが不良である場合は再度人証情報の書き換えを行ってテストに合格した場合に支給する。

なお、各人の認証に合格しない場合は不正なアクセスである可能性があるので人証情報の書き換えを拒絶する（S53）。

【0036】

人証情報の読み出しや書き換えがあったときには、不正使用などの異常が起こったときにその原因になっている場合があるので、ログを取って認証 IC カード自体に格納しておくことが好ましい。

このように、本実施例の認証 IC カードは、人証情報の読み出しや書き換えに立会人などの承認を要求するようにすることができるので、窃盗や拾得により取得した認証 IC カードを盗用したり改竄することができないばかりか、認証 IC カードの発行装置、読み取り装置、書き換え装置などを自由に扱える者であっても立会人等の承認がない限り使用することができないので、認証 IC カードの安全性は極めて高い。

【0037】

【発明の効果】

以上詳細に説明した通り、本発明の認証 IC カードは、発行時や人証情報の確認、書き換えに第 2 の人物の承認を要求するようにできるので、盗用等の危険が極めて小さく、安全性が高い。

【図面の簡単な説明】

【図 1】

本発明の 1 実施例の認証 IC カードの構成を示すブロック図である。

【図 2】

本実施例の認証 IC カード発行の手順を示す流れ図である。

【図 3】

本実施例の認証 IC カードに記録した人証情報読み出しの手順を示す流れ図である。

【図 4】

本実施例の認証 IC カードの人証情報書き換えの手順を示す流れ図である。

【符号の説明】

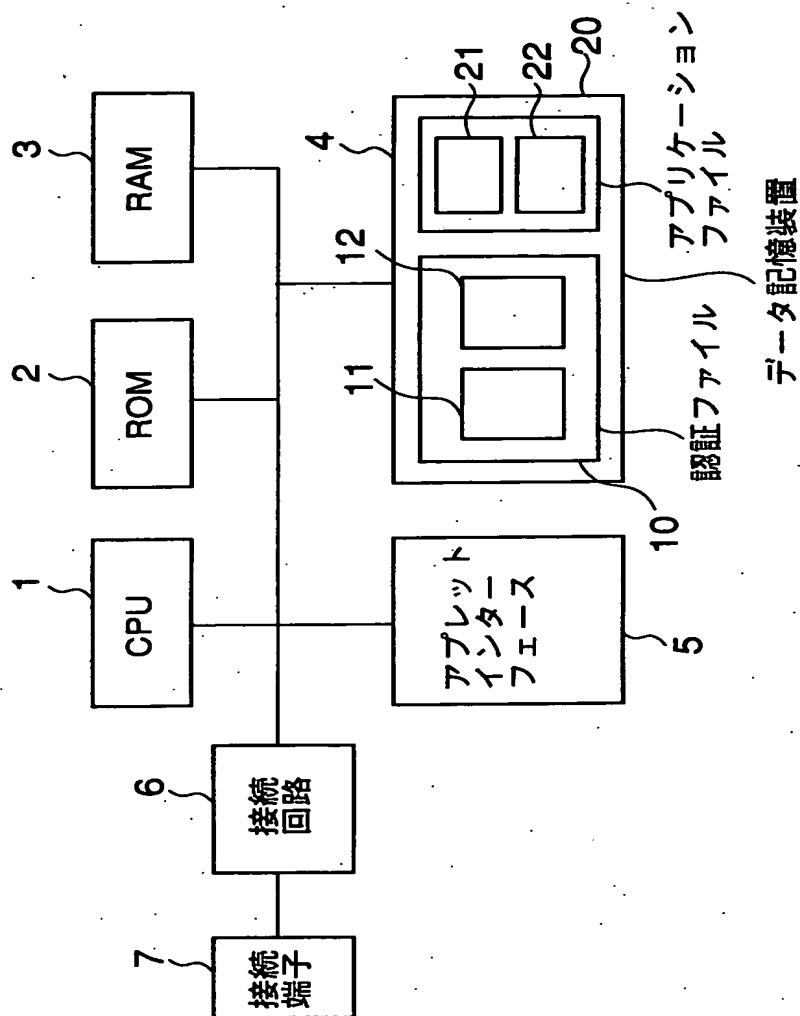
- 1 CPU
- 2 ROM
- 3 RAM

- 4 データ記憶装置
- 5 アプレットインターフェース
- 6 外部接続用接続回路
- 7 外部接続端子
- 10 認証ファイル
  - 11 第1人証ファイル
  - 12 第2人証ファイル
- 20 アプリケーションファイル
  - 21 第1作業ファイル
  - 22 第2作業ファイル



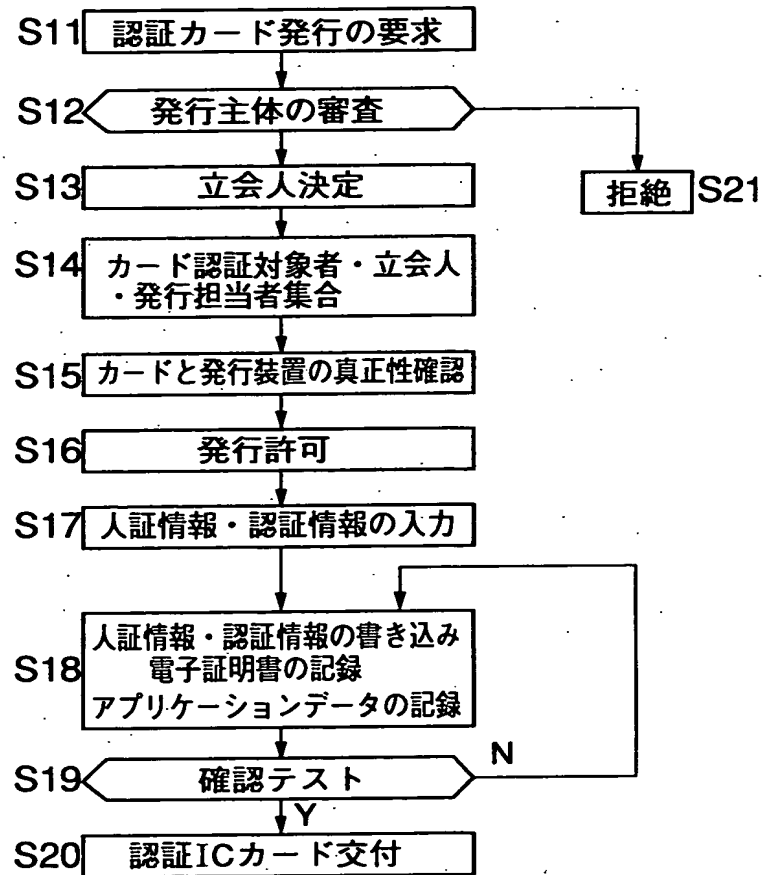
【書類名】 図面

【図 1】



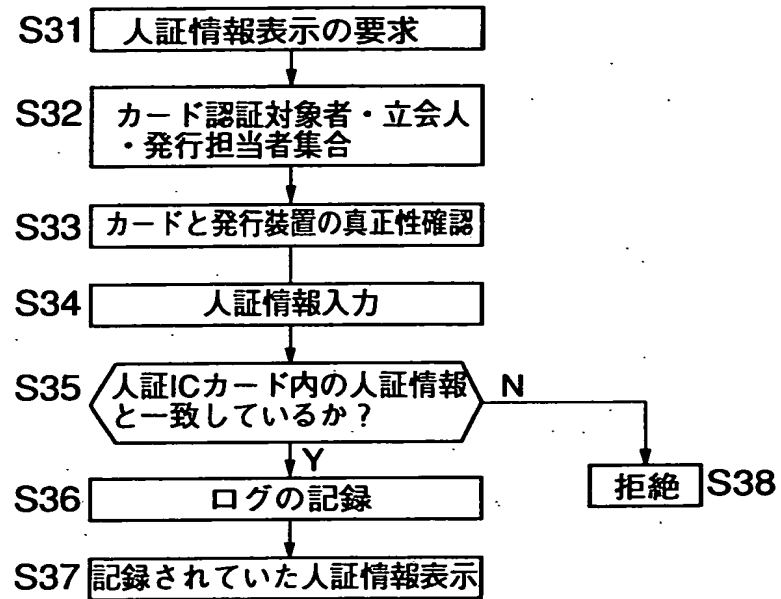
【図 2】

認証ICカード発行プロセス



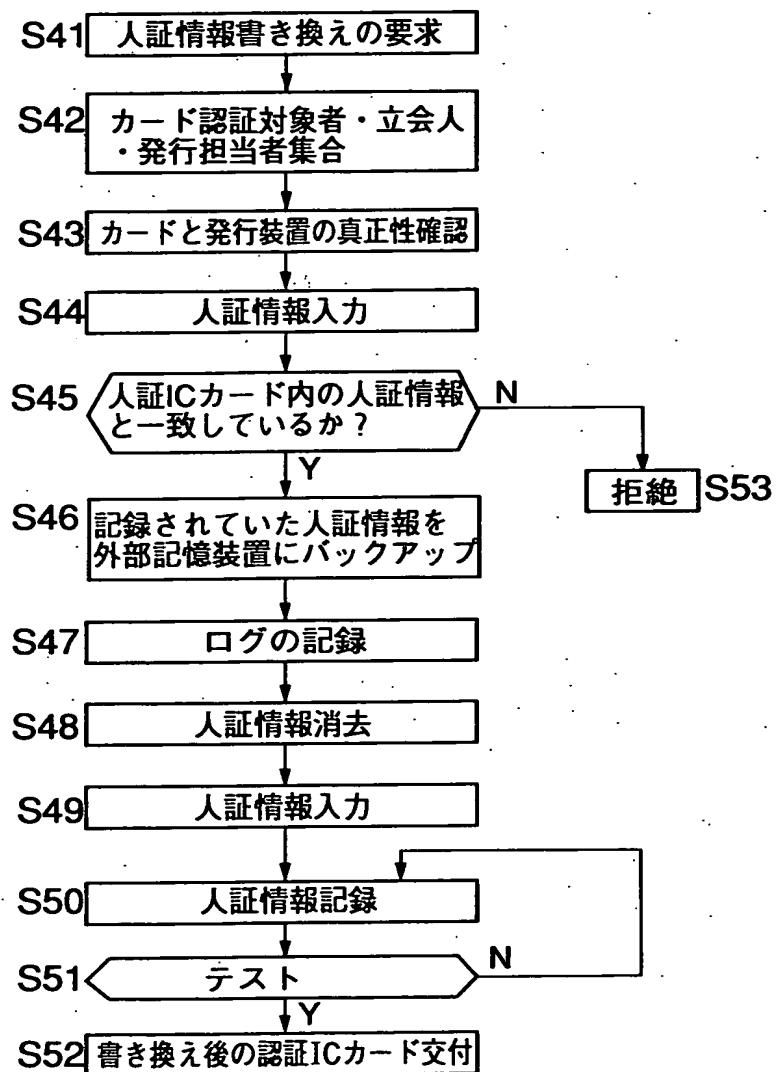
【図 3】

人証情報確認プロセス



【図 4】

人証情報書き換えプロセス



【書類名】 要約書

【要約】

【課題】 取引のセキュリティのために複数の取引対象についての資格者認証をする高度に安全な認証 IC カードを提供する。

【解決手段】 認証 IC カードに所有者の他に第 2 の人物の人証情報を格納し、認証 IC カードの真正性に係わるアクセスには本人以外に第 2 人物の認証を行えるようにする。

【選択図】 図 1

認定・付加情報

特許出願の番号	平成10年 特許願 第361752号
受付番号	59800827216
書類名	特許願
担当官	清水 直子 6175
作成日	平成11年 2月 1日

<認定情報・付加情報>

【提出日】	平成10年12月21日
-------	-------------

出 願 人 履 歴 情 報

識別番号

[398035796]

1. 変更年月日 1998年 5月 7日

[変更理由] 新規登録

住 所 千葉県八千代市勝田台南2丁目15番22号

氏 名 保倉 豊